

AMENDMENTS TO THE CLAIMS

The following listing of claims will replace all prior versions and listings of claims in the application.

1. (Currently Amended) A method for distributing encryption keys in a Wireless Local Area Network (WLAN), comprising:

receiving, by an authentication device, an authentication request containing identification information for identity authentication from a mobile host;

authenticating said mobile host according to said identification information;

if authentication fails, sending a message comprising ACCESS_REJECT information to said mobile host, and

if authentication succeeds, sending [[a]] key-related information M1 to an access point (AP) and a message comprising ACCESS_ACCEPT information to said mobile host, wherein the key-related information M1 includes property information associated with the mobile host, and said key-related information M1 is used to generate a key by said AP;

wherein if [[a]] key-related information M2 is comprised in said message comprising the ACCESS_ACCEPT information, said message comprising the ACCESS_ACCEPT information is encrypted, and said message comprising the ACCESS_ACCEPT information is used to obtain the key by the mobile host.;

~~said key-related information M1 is used to obtain a key by said AP, said message comprising the ACCESS_ACCEPT information is used to obtain the key by the mobile host.~~

2. (Currently Amended) The method for distributing encryption keys in the WLAN of claim 1 further comprising ~~wherein said key-related information M1 is the~~
~~corresponding property information searched by said authentication device according to~~
~~the identification information, the method of said AP obtaining the key comprises:~~

generating the key, by said AP, according to said property information associated
with the mobile host with a key generation algorithm; and ~~the method of said mobile~~
~~host obtaining the key comprises:~~

generating the key, by said mobile host, according to ~~[[the]]~~ property information
stored in the mobile host with the same key generation algorithm after said mobile host
receives said message comprising the ACCESS_ACCEPT information.

3. (Currently Amended) The method for distributing encryption keys in the WLAN of claim 1 further comprising ~~wherein said key-related information M1 is the~~
~~corresponding property information searched by said authentication device according to~~
~~the identification information, the method of said AP obtaining the key comprises:~~

generating the key, by said AP, with a key generation algorithm; wherein said
key-related information M2 ~~[[is]]~~ includes said key generated and encrypted by said AP
and is sent to said mobile host along with said ACCESS_ACCEPT message, said
mobile host obtaining the key through decrypting information M2 with said property
information.

4. (Cancelled)

5. (Cancelled)

6. (Currently amended) The method for distributing encryption keys in the WLAN of claim 1 wherein when receiving data packets encrypted with a key sent from the mobile host, said AP updates the key through the following steps of:

(a1) said AP generating a random number and generating a new key from said random number with any key generation algorithm;

(b1) said AP adding said random number to a key update message and then sending said message to said mobile host;

(c1) when receiving said key update message, said mobile host generating a new key from said random number contained in said key update message with the same key generation algorithm as that in step (a1);

(d1) said mobile host encrypting the data packets to be sent to said AP with said new key and then sending the encrypted data packets to said AP, during the encryption process, said mobile host adding an encryption identifier to said data packets and changing the value of said encryption identifier to indicate the communication key has been changed; and

(e1) when receiving the data packets from said mobile host, said AP determines whether to change the key according to value of said encryption identifier.

7. (Currently amended) The method for distributing encryption keys in the WLAN of claim 1 wherein in order to achieve encryption communication with the new key, when receiving the data packets encrypted with the key sent from said mobile host, said AP updates the key periodically or aperiodically through the following steps of:

(a2) said AP generating a new key in any way and encrypting said new key with the present key;

(b2) said AP adding the encrypted key to the key update message and then sending said message to said mobile host;

(c2) when receiving said key update message, said mobile host decrypting the new key contained in said key update message with the present key so as to obtain said new key;

(d2) said mobile host encrypting the data packets to be sent to said AP with said new key and then sending the encrypted data packets to said AP, during the encryption process, said mobile host adding an encryption identifier to said data packets and changing the value of said encryption identifier to indicate the communication key has been changed; and

(e2) when receiving the data packets from said mobile host, said AP determines whether to change the key according to value of said encryption identifier.

8. (Currently amended) The method for distributing encryption keys in the WLAN of claim 1 wherein when receiving the data packets encrypted with the key sent from said mobile host, said AP updates the key periodically or aperiodically through the following steps of:

(a3) said authentication device generating a random number which is used to generate a new key with the key generation algorithm, and then said authentication device sending said new key to said AP, and sending said random number to said mobile host via said AP;

(b3) said AP sending said key update message to said mobile host after receiving said new key;

(c3) when receiving said random number from said authentication device and said key update message from AP, said mobile host generating a new key from said random number with the same key generation algorithm as that in step (a3);

(d3) said mobile host encrypting the data packets to be sent to said AP with said new key and then sending the encrypted data packets to said AP, during the encryption process, said mobile host adding an encryption identifier to said data packets and changing the value of said encryption identifier to indicate the communication key has been changed; and

(e3) when receiving the data packets from said mobile host, said AP determines whether to change the key according to value of said encryption identifier.

9. (Currently amended) The method for distributing encryption keys in the WLAN of claim 1 wherein in order to achieve encryption communication with the new key, when receiving the data packets encrypted with the key sent from said mobile host, said AP updates the key periodically or aperiodically through the following steps of:

(a4) said AP generating a new key in any way and encrypting said new key with the present key, then sending said new key to said AP, whereas sending the encrypted new key to said mobile host via said AP;

(b4) after receiving said new key, said AP sending a key update message to said mobile host;

(c4) when receiving the encrypted key from said authentication device and said key update message from said AP, said mobile host decrypting the encrypted key with the present key to obtain a new key;

(d4) said mobile host encrypting the data packets to be sent to said AP with said new key and then sending the encrypted data packets to said AP, during the encryption process, said mobile host adding an encryption identifier to said data packets and changing the value of said encryption identifier to indicate the communication key has been changed; and

(e4) when receiving the data packets from said mobile host, said AP determines whether to change the key according to value of said encryption identifier.

10. (Previously Presented) The method for distributing encryption keys in the WLAN of claim 1 wherein said authentication device is an authentication server installed in external network.

11. (Previously Presented) The method for distributing encryption keys in the WLAN of claim 6 wherein said authentication device is an authentication server installed in external network.

12. (Previously Presented) The method for distributing encryption keys in the WLAN of claim 7 wherein said authentication device is an authentication server installed in external network.

13. (Previously Presented) The method for distributing encryption keys in the WLAN of claim 8 wherein said authentication device is an authentication server installed in external network.

14. (Previously Presented) The method for distributing encryption keys in the WLAN of claim 9 wherein said authentication device is an authentication server installed in external network.

15. (Previously Presented) The method for distributing encryption keys in the WLAN of claim 1 wherein said authentication device is a wireless gateway that connects said AP with external network.

16. (Previously Presented) The method for distributing encryption keys in the WLAN of claim 6 wherein said authentication device is a wireless gateway that connects said AP with external network.

17. (Previously Presented) The method for distributing encryption keys in the WLAN of claim 7 wherein said authentication device is a wireless gateway that connects said AP with external network.

18. (Previously Presented) The method for distributing encryption keys in the WLAN of claim 8 wherein said authentication device is a wireless gateway that connects said AP with external network.

19. (Previously Presented) The method for distributing encryption keys in the WLAN of claim 9 wherein said authentication device is a wireless gateway that connects said AP with external network.

20. (Previously Presented) The method for distributing encryption keys in the WLAN of claim 1 wherein said authentication device includes a wireless gateway and said authentication server installed in external network.

21. (Previously Presented) The method for distributing encryption keys in the WLAN of claim 6 wherein said authentication device includes a wireless gateway and said authentication server installed in external network.

22. (Previously Presented) The method for distributing encryption keys in the WLAN of claim 7 wherein said authentication device includes a wireless gateway and said authentication server installed in external network.

23. (Previously Presented) The method for distributing encryption keys in the WLAN of claim 8 wherein said authentication device includes a wireless gateway and said authentication server installed in external network.

24. (Previously Presented) The method for distributing encryption keys in the WLAN of claim 9 wherein said authentication device includes a wireless gateway and said authentication server installed in external network.

25. (Currently Amended) An authentication device, comprising:

a receiving module configured to receive an authentication request from a mobile host, said authentication request comprising identification information for identity authentication;

an authentication module configured to authenticate said mobile host according to said identification information;

a sending module configured to send a message comprising ACCESS_REJECT information to said mobile host if authentication fails, and send key-related information M1 to an access point (AP) for said AP to ~~obtain~~ generate a key according to said key-related information M1 and a message comprising ACCESS_ACCEPT information to said mobile host for said mobile host to obtain the key according to said message comprising the ACCESS_ACCEPT information, if authentication succeeds, wherein the key-related information M1 includes property information associated with the mobile host.

26. (Currently Amended) A system, comprising:

a mobile host, an authentication device, and an access point (AP);

said authentication device configured to receive an authentication request from said mobile host, said authentication request comprising identification information for identity authentication, to authenticate said mobile host according to said identification information, to send an ACCESS_REJECT message to said mobile host if authentication fails, to send ~~[[a]]~~ key-related information M1 to ~~[[an]]~~ the access point (AP) and to send a message comprising ACCESS_ACCEPT information to said mobile host if authentication succeeds, wherein the key-related information M1 includes property information associated with the mobile host;

said mobile host configured to send an authentication request containing identification information for identity authentication, and to ~~obtain~~ generate a key according to said message comprising ACCESS_ACCEPT information;

said AP configured to receive said key-related information M1 and obtain the key according to said key-related information M1.